REMARKS

In the Office Action, the Examiner rejected the claims under 35 USC §102 and 35 USC §103. In addition, claims 5-7 and 32 have been rejected under 35 USC §112. The claims have been amended to further clarify the subject matter regarded as the invention. The rejections are fully traversed below. Claims 1-53 remain pending.

Reconsideration of the application is respectfully requested based on the following remarks.

REJECTION OF CLAIMS UNDER 35 USC §102

In the Office Action, the Examiner has rejected claims 1-10, 13-36, and 38-53 under 35 USC §102(e) as being anticipated by Yokote, U.S. Patent Pub. No. 2002/0147820, ('Yokote' hereinafter). This rejection is fully traversed below.

Yokote discloses a method for implementing IP security in Mobile IP networks. See title. More particularly, a sending node initiates the establishment of a security association for a receiving node. See Abstract. For instance, as shown in FIGs. 6 and 7 of Yokote, a Correspondent Node (CN) initiates the establishment of a security association for a Mobile Node by contacting a Ticket Granting Server (TGS). It is also important to note that once the TGS generates a session key, the TGS transmits the session key to the CN, which then transmits the session key to the Mobile Node. In other words, the Mobile Node does not need to generate or otherwise derive the session key.

In contrast, the claimed invention does not transmit a session key. Rather, the entity communicating with the server separately derives the session key. For instance, as recited in claim 1, a server may derive key information (not the final key) and send the key information to the Home Agent. The Home Agent may then derive a key to be shared between the Mobile Node and the Home Agent from the key information. It is also important to note that, as recited in claim 10, the Home Agent does not transmit the key to the Mobile Node. Rather, the Mobile Node separately derives the key. As a result, the pending claims provide a more secure mechanism for generating session keys than the cited art.

Moreover, the claimed invention does not require a sending node to initiate the

establishment of a security association for a receiving node. Rather, the claimed invention enables a sending node to initiate the establishment of a security association on its own behalf. Yokote fails to disclose or suggest a sending node initiating the establishment of a security association.

The remaining independent claims are patentable for similar reasons. The dependent claims depend from one of the independent claims and are therefore patentable for at least the same reasons. However, the dependent claims recite additional limitations that further distinguish them from Yokote.

For example, with respect to claim 15, the Examiner asserts that Yokote eaches "wherein the Mobile Node is to derive the shared key from a second set of key information stored at the Mobile Node," citing paragraph 0061. However, Applicant was unable to find any reference to a Mobile Node in this paragraph. Therefore, Yokote fails to disclose or suggest a Mobile Node deriving a shared key from a second set of key information stored at the Mobile Node. In fact, Applicant respectfully asserts that Yokote fails to disclose or suggest a Mobile Node deriving a shared key in any manner. Applicant therefore respectfully submits that claim 15 is patentable over Yokote.

Moreover, with respect to claim 21, the Examiner asserts that Yokote teaches that the registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent, citing Fig. 6, ref. num. S6-3. However, ref. num. S6-3 actually illustrates a TGS creating a session key in order to transmit the session key to a Correspondent Node. In fact, ref. num. S6-3 fails to disclose or suggest sending a registration reply in any manner. Moreover, S6-3 fails to show a Mobile Node. Accordingly, Applicant respectfully submits that claim 21 is patentable over Yokote.

As yet another example, claim 31 recites that "the key information is derived from a password associated with the Mobile Node." Although Yokote discloses that a user enters a username, Applicant respectfully asserts that Yokote fails to disclose or suggest deriving key information from the username, enabling a shared key between a Mobile Node and a Home Agent to be derived from the key information. Accordingly, Applicant respectfully submits that Yokote fails to anticipate claim 31.

The additional limitations recited in the independent claims or the dependent claims are not further discussed, as the above discussed limitations are clearly sufficient to distinguish the claimed invention from the cited reference. Thus, it is respectfully requested that the Examiner withdraw the rejection of the claims under 35 USC §102.

Atty Docket No.: CISCP334/6994   - 17 -   Application No. 10/635,882

PAGE 19/21 * RCVD AT 6/13/2007 7:42:08 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/4 * DNIS:2738300 * CSID:5106630920 * DURATION (mm-ss):05-18

REJECTION OF CLAIMS UNDER 35 USC §103

In the Office Action, the Examiner has rejected claims 11, 12, and 37 under 35 USC §103(A) as being unpatentable over Yokote in view of Abrol et al, U.S. Patent. No. 6,785,823, ('Abrol' hereinafter). This rejection is fully traversed below.

As set forth above, Yokote teaches the transmission of a session key. As such, Yokote teaches away from the claimed invention, which does not transmit a session key between entities. As such, Yokote teaches away from the independent derivation of the session key by entities such as the Home Agent and Mobile Node, as recited in claims 1 and 10, respectively.

The Examiner further cites Abrol. However, Abrol fails to cure the deficiencies of Yokote. It is also important to note that although Abrol does disclose a CHAP Challenge and a CHAP Response, Abrol fails to disclose or suggest a registration request that includes a CHAP Challenge or CHAP Response. In fact, FIG. 2, cited by the Examiner, shows that a Mobile IP registration request is transmitted separately from the CHAP Challenge and CHAP Response. More particularly, The Mobile IP registration request is transmitted after the CHAP Challenge/Response messages are transmitted. As a result, the combination of the cited references would fail to achieve the desired result.

The cited references, separately or in combination, fail to disclose or suggest the disadvantages of transmitting a session key between entities. Moreover, the cited references fail to disclose or suggest a solution to such a problem. Accordingly, Applicant respectfully submits that 11, 12, and 37 are patentable over the cited references.

SUMMARY

If there are any issues remaining which the Examiner believes could be resolved through either a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned attorney at the telephone number listed below.

Applicants hereby petition for an extension of time which may be required to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 50-0388 (Order No. CISCP334).

Respectfully submitted,
BEYER WEAVER LLP
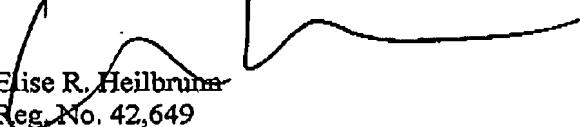
Elise R. Heilbrunn
Reg. No. 42,649

P.O. Box 70250
Oakland, CA 94612-0250

Tel: (510) 663-1100

Atty Docket No.: CISCP334/6994   - 19 -   Application No. 10/635,882

PAGE 21/21 * RCVD AT 6/13/2007 7:42:08 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/4 * DNIS:2738300 * CSID:5106630920 * DURATION (mm-ss):05-18